

## IN THE SPECIFICATION

Please insert the following paragraph after the subtitle "Detailed Description of the Invention" and prior to paragraph [0039]. No new matter has been entered.

In an aspect, a countermeasure method for resisting security attacks on a processing unit is provided. The method using a key to perform a defined cryptographic function, the method comprising the following steps: a) obtaining the key and a random value  $r$ ; b) obtaining a set of  $n$  random input values  $min1, \dots minn$ ; c) defining a masked function by masking the defined cryptographic function with the value  $min1 \wedge \dots \wedge minn$ ; d) masking the key with the random value  $r$  to define the value  $mkey$ ; e) obtaining a set of random values  $m1, \dots mn-1$ ; f) defining a value  $mn$  to be  $r \wedge min1 \wedge \dots \wedge minn \wedge m1 \wedge \dots \wedge mn-1$ ; and g) using the values  $m1, \dots, mn$  and  $mkey$  to define input for the masked function.

Please amend paragraph [0043] of the specification as follows. No new matter has been entered.

[0043] Further, the preferred embodiment may be implemented as a computer program product that includes code to carry out the steps in the process described. The preferred embodiment may be implemented as a computer system (which includes a subsystem or system defined to work in conjunction with other systems) for encryption that includes elements that execute the functions as described. The computer system of the preferred embodiment may be defined by, and the computer program product may be embodied in, ~~signals carried by networks, including the Internet or may be embodied in~~ storage media such as magnetic, electronic or optical storage media.